

2-arcs of maximal size in the affine and the projective Hjelmslev plane over \mathbb{Z}_{25}

Michael Kiermaier, Matthias Koch and Sascha Kurz

January 20, 2014

Abstract

It is shown that the maximal size of a 2-arc in the projective Hjelmslev plane over \mathbb{Z}_{25} is 21, and the $(21, 2)$ -arc is unique up to isomorphism. Furthermore, all maximal $(20, 2)$ -arcs in the affine Hjelmslev plane over \mathbb{Z}_{25} are classified up to isomorphism.

1 Introduction

It is well known that a Desarguesian projective plane of order q admits a 2-arc of size $q + 2$ if and only if q is even. These 2-arcs are called *hyperovals*. The biggest 2-arcs in the Desarguesian projective planes of odd order q have size $q + 1$ and are called *ovals*.

For a projective Hjelmslev plane over a chain ring R of composition length 2 and size q^2 , the situation is somewhat similar: In $\text{PHG}(2, R)$ there exists a hyperoval – that is a 2-arc of size $q^2 + q + 1$ – if and only if R is a Galois ring of size q^2 with q even, see [7, 6]. For the case q odd and R not a Galois ring it was recently shown that the maximum size $m_2(R)$ of a 2-arc is q^2 , see [4].

In the remaining cases, the situation is less clear. For even q and R not a Galois ring, it is known that the maximum possible size of a 2-arc is lower bounded by $q^2 + 2$ [4] and upper bounded by $q^2 + q$ [6]. The last case q odd and R a Galois ring currently is the least satisfactory one. Besides the upper bound q^2 , only the lower bound $\left(\frac{q+1}{2}\right)^2$ is known [4], leaving a comparatively large gap.

The current state of the lower and upper bounds on the maximal size of

a 2-arc for general q is summarized in the following table:

$m_2(R)$		R	
		Galois ring	not a Galois ring
q	even	$q^2 + q + 1$	$q^2 + 2 \leq \cdot \leq q^2 + q$
	odd	$\left(\frac{q+1}{2}\right)^2 \leq \cdot \leq q^2$	q^2

In the open cases for $\#R \leq 16$ the exact values were determined computationally [8, 3]. The ring $R = \mathbb{Z}_{25}$ is the smallest one where the exact value $m_2(R)$ was not known beforehand. In [2] the first 2-arc in $\text{PHG}(2, \mathbb{Z}_{25})$ of size 20 was found. This was the biggest known 2-arc until in [9] a 2-arc of size 21 was given. The main result of this paper is:

Theorem 1.1 *The maximum size of a 2-arc in $\text{PHG}(2, \mathbb{Z}_{25})$ is 21. The $(21, 2)$ -arc is unique up to isomorphism.*

The projective Hjelmslev plane over \mathbb{Z}_{25} has 775 points, so the search space for arcs of size 21 or 22 is way too big to allow a direct attack by a backtrack search. Therefore, special computational methods had to be developed.

In Section 2, we give a brief introduction to finite chain rings and coordinate Hjelmslev planes. For details, see for example [21, 22]¹ and [6], respectively. For the computation, two independent approaches are used: In Section 3, in a first step the possible images of a $(22, 2)$ -arc in the factor plane are computed up to isomorphism, and in the second step the preimages are investigated. In Section 4 first the $(20, 2)$ -arcs in the affine plane are classified and then checked for extendability to a $(22, 2)$ -arc in the projective plane. In Section 5, further computational results are summarized, and the maximum size of a 2-arc of a given maximum point class multiplicity is determined for the projective Hjelmslev planes over \mathbb{Z}_{25} and \mathbb{S}_5 , which is the other chain ring of composition length 2 and size 25.

Computational nonexistence- and uniqueness proofs using highly non-trivial algorithms are always a delicate matter, since already a subtle glitch in the implementation may very well cause a totally wrong result. For that reason we put a lot of effort on assuring the correctness of our implementations. The maximality and uniqueness of the $(21, 2)$ -arc was achieved independently by our two approaches. Furthermore, both approaches independently report the number of the $\text{PGL}(3, R)\downarrow$ -isomorphism classes of $(20, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ as 488.

¹In these two references, finite chain rings are called *Galois-Eisenstein-Ore-rings* (*GEO-rings*).

2 Notation and Preliminaries

2.1 Finite chain rings

Let R be a finite ring.² R is called *chain ring* if the lattice of the left-ideals is a chain. A chain ring is necessarily local, so there is a unique maximum ideal $N = \text{rad}(R)$. It can be shown that N is a principal ideal. Because R is finite, the quotient ring R/N is isomorphic to a finite field \mathbb{F}_q of order $q = p^r$ with p prime. R/N is called the *residue class field* of R .

We will need the projection $\phi : R \rightarrow \mathbb{F}_q$, $a \mapsto a \bmod N$, which is a surjective ring homomorphism. The number of ideals of R reduced by 1 is the composition length of R , considered as a left module ${}_R R$. This number will be denoted by m . The order of R is q^m .

An important subclass of the finite chain rings are the *Galois rings*. Their definition is a slight generalization of the construction of finite fields via irreducible polynomials:

Let p be prime, r and m positive integers, $q = p^r$ and $f \in \mathbb{Z}_{p^m}[X]$ be a monic polynomial of degree r such that the image of f modulo p is irreducible in $\mathbb{F}_p[X]$. Then the *Galois ring* of order q^m and characteristic p^m is defined as

$$\text{GR}(q^m, p^m) = \mathbb{Z}_{p^m}[X]/(f).$$

Up to isomorphism, the definition is independent of the particular choice of f . The symbols p , q , r and m are consistent with the earlier definitions: $\text{GR}(q^m, p^m) / \text{rad}(\text{GR}(q^m, p^m)) \cong \mathbb{F}_q$ and the composition length of $\text{GR}(q^m, p^m)$ is m . Furthermore, the class of the Galois rings contains the finite fields and the integer residue class rings modulo a prime power: $\text{GR}(p^m, p^m) \cong \mathbb{Z}_{p^m}$ and $\text{GR}(p^r, p) \cong \mathbb{F}_{p^r}$.

The finite fields are exactly the finite chain rings of composition length 1. In the following we assume that R is a finite chain ring of composition length 2. The isomorphism types of these rings are known[23, 21, 1]: For a fixed size $q = p^r$ of the residue field of R there are $r+1$ possible isomorphism types for R . One is the Galois ring $\text{GR}(q^2, p^2)$ of characteristic p^2 , and the remaining r ones are all of characteristic p and not isomorphic to a Galois ring. Among the latter r possibilities there is a single commutative ring, which is $\mathbb{S}_q = \mathbb{F}_q[X]/(X^2)$.

In particular, up to isomorphism the only chain rings of size 25 and composition length 2 are \mathbb{Z}_{25} and $\mathbb{S}_5 = \mathbb{F}_5[X]/(X^2)$.

2.2 Affine and projective coordinate Hjelmslev planes

The *projective Hjelmslev plane* $\text{PHG}(2, R)$ over a finite chain ring R is defined as follows: The point set $\mathcal{P}(\text{PHG}(2, R))$ [line set $\mathcal{L}(\text{PHG}(2, R))$] is the

²Rings are assumed to contain an identity element $1 \neq 0$ and to be associative, but not necessarily commutative.

set of the free rank 1 [rank 2] right submodules of the right R -module R^3 , and the incidence relation is given by set inclusion. For a point x a vector $\mathbf{v} \in R^3$ with $x = \mathbf{v}R$ is called *coordinate vector* of x . x has $\#R^\times = q(q-1)$ coordinate vectors. There is a unique coordinate vector of x whose first unit entry is 1.

The *affine Hjelmslev plane* $\text{AHG}(2, R)$ over a finite chain ring R is defined as follows: The point set $\mathcal{P}(\text{AHG}(2, R))$ is the set of the vectors in R^2 , and the line set $\mathcal{L}(\text{AHG}(2, R))$ is the set of all cosets of free rank 1 submodules of the right R -module R^2 . The incidence relation is given by set membership.

For the number of points and lines we have

$$\#\mathcal{P}(\text{PHG}(2, R)) = \#\mathcal{L}(\text{PHG}(2, R)) = \frac{q^3 - 1}{q - 1}q^2 \quad \text{and}$$

$$\#\mathcal{P}(\text{AHG}(2, R)) = q^4, \quad \#\mathcal{L}(\text{AHG}(2, R)) = q^3(q + 1).$$

The projective and affine Hjelmslev planes share a lot of structure which will be described simultaneously: Let $(\mathcal{H}, \mathcal{G})$ be either $(\text{PHG}(2, R), \text{PG}(2, \mathbb{F}_q))$ or $(\text{AHG}(2, R), \text{AG}(2, \mathbb{F}_q))$. For a consistent description, in the following we identify a line L of $\text{PHG}(2, R)$ with the set of points incident with L , so that the incidence relation of both $\text{PHG}(2, R)$ and $\text{AHG}(2, R)$ is given by set membership.

In contrast to classical planes, in Hjelmslev planes it may happen that two distinct lines meet each other in more than a single point. More precisely, there is more than one line passing through points x and y of \mathcal{H} if and only if $\phi(x) = \phi(y)$, where the mapping ϕ is extended from R to $\mathcal{P}(\mathcal{H})$. Each preimage $\phi^{-1}(z)$ with $z \in \mathcal{P}(\mathcal{G})$ is called *point class*. For $x \in \mathcal{P}(\mathcal{H})$, the point class $\phi^{-1}(\phi(x))$ containing x is denoted by $[x]$. Similarly, two lines L_1 and L_2 of \mathcal{H} intersect in more than one point if and only if $\phi(L_1) = \phi(L_2)$. The preimages $\phi^{-1}(l)$ with $l \in \mathcal{L}(\mathcal{G})$ are called *line classes*. For $L \in \mathcal{L}(\mathcal{H})$, the line class $\phi^{-1}(\phi(L))$ containing L is denoted by $[L]$. So by our definition, a line class $[L]$ is a set of points.

Similarly to the classical case, the projective and the affine Hjelmslev plane over R are tightly related: By the mapping $\mathcal{P}(\text{AHG}(2, R)) \rightarrow \mathcal{P}(\text{PHG}(2, R))$, $\mathbf{v} \mapsto (1, \mathbf{v})R$, the affine Hjelmslev plane is embedded in the projective Hjelmslev plane. We will refer to this embedding as the *standard embedding*. The points in $\text{PHG}(2, R)$ not contained in the image of $\text{AHG}(2, R)$ form a line class. This line class is called *line class at infinity* and given by all points $\mathbf{v}R$ such that the first component of \mathbf{v} is not a unit. On the other hand, removing a line class $[L]$ from $\text{PHG}(2, R)$ yields a plane isomorphic to $\text{AHG}(2, R)$, and $[L]$ is its line class at infinity.

There is also an axiomatic definition of projective and affine Hjelmslev planes which does not rely on an underlying chain ring [12, 18]. This definition is more general than the one given above: Not every axiomatically defined Hjelmslev plane can be coordinatized over a finite chain ring. For

that reason, the Hjelmslev planes $\text{PHG}(2, R)$ and $\text{AHG}(2, R)$ are also called *coordinate* Hjelmslev planes. The axiomatic definition of an affine Hjelmslev plane involves a *parallelism*, which is an equivalence relation on the set of lines satisfying Euclid's parallel axiom. In contrast to classical affine planes, in general the parallelism of an affine Hjelmslev plane is not uniquely determined by its underlying incidence structure. For a coordinate affine Hjelmslev plane $\text{AHG}(2, R)$ embedded in $\text{PHG}(2, R)$, each line L contained in the line class at infinity induces a parallelism in the following way: Two lines in $\mathcal{L}(\text{AHG}(2, R))$ are called parallel if and only if they pass through the same point on L . Using the standard embedding, we will call the parallelism induced by the line $(1, 0, 0)^\perp$ the *standard parallelism*.

2.3 Induced subgeometries

Because $\phi : \mathcal{P}(\mathcal{H}) \rightarrow \mathcal{P}(\mathcal{G})$ maps lines to lines, the geometry of the point classes and the line classes with incidence given by the subset relation is isomorphic to the plane \mathcal{G} . This plane is called *factor plane* of \mathcal{H} .

The restriction of the geometry \mathcal{H} to a single point class $[x]$ is isomorphic to the affine plane $\text{AG}(2, \mathbb{F}_q)$. It will be denoted by $\Pi_{[x]}$. Each line in one of these affine geometries is called *line segment* when considered as a subset of $\mathcal{P}(\mathcal{H})$.

Now let $L \in \mathcal{L}(\mathcal{H})$ be a line. Let $[x]$ be a point class incident with $[L]$. Then $L \cap [x]$ is a line segment contained in $[x]$. The set of all line segments P arising as $L' \cap [x]$ with $L' \in [L]$ forms a parallel class of lines in the affine plane on $[x]$. In this way, the parallel classes on $[x]$ are in bijection with the line classes incident with $[x]$ in the factor plane. We will say that the line class $[L]$ *determines* the parallel class P , and that the parallel class P *determines* the line class $[L]$. Since a parallel class in $\Pi_{[x]}$ is already determined by a single line or by the unique line passing through a pair of distinct points in $[x]$, we will also use the formulation that the line class $[L]$ is determined by a line segment or by a pair of distinct points.

In the projective case $\mathcal{H} = \text{PHG}(2, R)$ the line segments determined by a line class form a geometry in the following sense: Let

$$\mathfrak{P} = \{\text{all line segments determined by } [L]\} \cup \{\infty\}.$$

For each point class $[x]$ incident with $[L]$ we define

$$L_{[x]} = \{\text{all line segments determined by } [L] \text{ contained in } [x]\} \cup \{\infty\}$$

and $\mathfrak{L} = \{L' : L' \in \mathcal{L}(\mathcal{H}), L' \subset [L]\} \cup \{L_{[x]} : x \in [L]\}$. Then the geometry $\Pi_{[L]}$ consisting of the point set \mathfrak{P} and the line set \mathfrak{L} with the incidence relation defined in the obvious way³ is isomorphic to the projective plane $\text{PG}(2, \mathbb{F}_q)$.

³Let $X \in \mathfrak{L}$. A line segment S is incident with X if $S \subseteq L$, and the point ∞ is incident with X if $\infty \in L$.

2.4 Collineations

A *collineation* of a point-line geometry is a bijection on the point set mapping lines to lines. As usual, two multisets of points are called *isomorphic* if they are contained in the same orbit under the action of the collineation group. In this article we do not require that a collineation of an affine Hjelmslev plane preserves its parallelism. The reason for this is that the group of collineations will be used to reduce the search space of the maximal arc problem, which does not depend on the parallelism.

The group $\Gamma\mathrm{L}(3, R)$ consists of all elements (A, σ) with $A \in \mathrm{GL}(3, R)$ and $\sigma \in \mathrm{Aut}(R)$. The multiplication in $\Gamma\mathrm{L}(3, R)$ is given by $(A, \sigma) \cdot (B, \rho) = (A\sigma(B), \sigma\rho)$. Thus $\Gamma\mathrm{L}(3, R)$ is a semidirect product $\mathrm{GL}(3, R) \rtimes \mathrm{Aut}(R)$. $\Gamma\mathrm{L}(3, R)$ acts on the set of points of \mathcal{H} via $(\mathbf{A}, \sigma) \cdot \mathbf{v}R = \mathbf{A}\sigma(\mathbf{v})R$. The kernel of this group action is $N = \{(\mathbf{I}_3\lambda^{-1}, a \mapsto \lambda a\lambda^{-1}) : \lambda \in R^*\}$, where \mathbf{I}_3 denotes the 3×3 unit matrix. Now the *projective semilinear group* $\mathrm{P}\Gamma\mathrm{L}(3, R)$ is defined as the factor group $\Gamma\mathrm{L}(3, R)/N$ and acts faithfully on $\mathcal{P}(\mathcal{H})$. By the fundamental theorem of projective Hjelmslev geometry [14], $\mathrm{P}\Gamma\mathrm{L}(3, R)$ is the group of collineations of $\mathrm{PHG}(2, R)$.

Starting with $\mathrm{GL}(3, R)$ instead of $\Gamma\mathrm{L}(3, R)$, the kernel of the group action on $\mathcal{P}(\mathcal{H})$ is $N = \mathbf{I}_3 Z(R^*)$, where $Z(R^*)$ is the center of the unit group of R . The *projective linear group* $\mathrm{PGL}(3, R)$ is defined as $\mathrm{PG}(3, R)/N$. It is worth mentioning that while the index of $\mathrm{GL}(3, R)$ in $\Gamma\mathrm{L}(3, R)$ is $\#\mathrm{Aut}(R)$, the index of $\mathrm{PGL}(3, R)$ in $\mathrm{P}\Gamma\mathrm{L}(3, R)$ is only $[\mathrm{Aut}(R) : \mathrm{Inn}(R)]$, where $\mathrm{Inn}(R)$ denotes the group of inner automorphisms of R . $\mathrm{PGL}(3, R)$ acts transitively on the set of ordered quadruples of points in general position (no 2 points in the same point class, no 3 collinear non-empty point classes) [1, Thm. 17]. This group action is regular if and only if R is commutative.

In the following it is assumed that $\mathrm{AHG}(2, R)$ is embedded into $\mathrm{PHG}(2, R)$ by the standard embedding. It is clear that all $\sigma \in \mathrm{P}\Gamma\mathrm{L}(3, R)$ fixing $\mathrm{AHG}(2, R)$ as a set give rise to a collineation of $\mathrm{AHG}(2, R)$, which will be denoted by $\sigma\downarrow$. The stabilizer of $\mathrm{AHG}(2, R)$ in $\mathrm{P}\Gamma\mathrm{L}(3, R)$ will be denoted by $\mathrm{P}\Gamma\mathrm{L}(3, R)_\infty$, and the set of induced collineations of $\mathrm{AHG}(2, R)$ will be denoted by $\mathrm{P}\Gamma\mathrm{L}(3, R)\downarrow$. The symbols $\mathrm{PGL}(3, R)_\infty$ and $\mathrm{PGL}(3, R)\downarrow$ are defined analogously. It can be checked that the restriction $\downarrow : \mathrm{P}\Gamma\mathrm{L}(3, R)_\infty \rightarrow \mathrm{P}\Gamma\mathrm{L}(3, R)\downarrow$ is a bijection. In general, $\mathrm{P}\Gamma\mathrm{L}(3, R)\downarrow$ is not the full collineation group of $\mathrm{AHG}(2, R)$: For example $\mathrm{P}\Gamma\mathrm{L}(3, \mathbb{Z}_9)\downarrow = \mathrm{PGL}(3, \mathbb{Z}_9)\downarrow$ has index 3 in the full collineation group of $\mathrm{AHG}(2, \mathbb{Z}_9)$.

Let $\rho : \mathbf{v}R \mapsto \mathbf{A}\sigma(\mathbf{v})R$ be an element of $\mathrm{P}\Gamma\mathrm{L}(3, R)_\infty$, where $(\mathbf{A}, \sigma) \in \Gamma\mathrm{L}(3, R)$ with $\mathbf{A} \in \mathrm{GL}(3, R)$ and $\sigma \in \mathrm{Aut}(R)$ is a representative of an element of $\mathrm{P}\Gamma\mathrm{L}(3, R)$. Then we may choose \mathbf{A} in the form

$$\mathbf{A} = \begin{pmatrix} 1 & c_1 & c_2 \\ b_1 & a_1 & a_2 \\ b_2 & a_3 & a_4 \end{pmatrix}$$

with $a_1, a_2, a_3, a_4, b_1, b_2 \in R$ and $c_1, c_2 \in \text{rad}(R)$. Let $\mathbf{A}' = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$, $\mathbf{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ and $\mathbf{c} = (c_1, c_2) \in \text{rad}(R) \times \text{rad}(R)$. Since \mathbf{A} is invertible, so is \mathbf{A}' .

By the standard embedding each element of $\text{AHG}(2, R)$ has the form $\begin{pmatrix} 1 \\ \mathbf{v} \end{pmatrix}$ with $\mathbf{v} \in R^2$. It holds $\rho \left(\begin{pmatrix} 1 \\ \mathbf{v} \end{pmatrix} \right) = \mathbf{A} \begin{pmatrix} 1 \\ \sigma(\mathbf{v}) \end{pmatrix} = \begin{pmatrix} 1 + \mathbf{c}\sigma(\mathbf{v}) \\ \mathbf{A}'\sigma(\mathbf{v}) + \mathbf{b} \end{pmatrix}$. Because of $\mathbf{c} \in \text{rad}(R) \times \text{rad}(R)$, $(1 + \mathbf{c}\sigma(\mathbf{v}))^{-1} = (1 - \mathbf{c}\sigma(\mathbf{v}))$, so $\rho \left(\begin{pmatrix} 1 \\ \mathbf{v} \end{pmatrix} \right) R = \begin{pmatrix} 1 \\ (\mathbf{A}'\sigma(\mathbf{v}) + \mathbf{b})(1 - \mathbf{c}\sigma(\mathbf{v})) \end{pmatrix} R$. So in affine coordinates $\rho \downarrow$ maps \mathbf{v} to $-\mathbf{A}'\sigma(\mathbf{v})\mathbf{c}\sigma(\mathbf{v}) + (\mathbf{A}' - \mathbf{b}\mathbf{c})\sigma(\mathbf{v}) + \mathbf{b}$.

$\rho \downarrow$ preserves the standard parallelism if and only if $\mathbf{c} = \mathbf{0}$. Hence the mappings in $\text{PTL}(3, R) \downarrow$ preserving the standard parallelism are given by the group $\text{AFL}(2, R)$ consisting of all mappings $R^2 \rightarrow R^2, \mathbf{v} \mapsto \mathbf{A}\sigma(\mathbf{v}) + \mathbf{b}$ with $\mathbf{A} \in \text{GL}(2, R)$, $\sigma \in \text{Aut}(R)$ and $\mathbf{b} \in R^2$. It holds

$$\begin{aligned} \# \text{AFL}(2, R) &= (q-1)^2 q^9 (q+1) \cdot \# \text{Aut}(R), \\ [\text{PTL}(3, R) \downarrow : \text{AFL}(2, R)] &= q^2 \quad \text{and} \\ [\text{PTL}(3, R) : \text{PTL}(3, R) \downarrow] &= q^2 + q + 1. \end{aligned}$$

For example the ring of our main interest $R = \mathbb{Z}_{25}$ has only the trivial automorphism. So $\text{PTL}(3, \mathbb{Z}_{25}) = \text{PGL}(3, \mathbb{Z}_{25})$, $\text{AFL}(2, \mathbb{Z}_{25}) = \text{AGL}(2, \mathbb{Z}_{25})$, $\# \text{PGL}(3, \mathbb{Z}_{25}) = 145312500000$, $\# \text{PGL}(3, \mathbb{Z}_{25}) \downarrow = 4687500000$ and $\# \text{AGL}(2, \mathbb{Z}_{25}) = 1875000000$. We used the graph isomorphism package `nauty` [20] to see that $\text{PGL}(3, \mathbb{Z}_{25}) \downarrow$ is in fact the full collineation group of $\text{AHG}(2, \mathbb{Z}_{25})$.

2.5 Arcs

For any geometry and any $n \in \mathbb{N}$, a multiset of points \mathfrak{k} of size n is called (n, w) -arc, if no $w+1$ elements of \mathfrak{k} are collinear⁴. We denote by $m_w(R)$ the maximum size of a w -arc in the projective Hjelmslev plane $\text{PHG}(2, R)$. There is an online table [10] for known lower bounds on $m_w(R)$.

We want to mention that the literature is inconsistent about allowing an arc to be a proper multiset. Our definition is motivated by the connection to coding theory [5] where the possibly repeated columns of a generator matrix are interpreted as coordinate vectors in projective Hjelmslev geometries. This article is about 2-arcs, where the different possible definitions do not matter: The only proper multiset which is a 2-arc consists of a single point of multiplicity 2.

For an arc \mathfrak{K} and a point set $X \subseteq \mathcal{P}$, the size $\#(X \cap \mathfrak{K})$ is called *multiplicity* of X . In this way, multiplicities are declared for point classes and

⁴Of course we have to respect multiplicities for counting the number of collinear points.

line classes. A point class of multiplicity u will simply be called u -class. Furthermore, the maximum value of u such that there is a u -class will be denoted by $u(\mathfrak{K})$. It is the *maximum point class multiplicity* of \mathfrak{K} .

3 Computation via the images in the factor plane

We define the map $\Phi : \mathbb{N}^{\mathcal{P}(\text{PHG}(2,R))} \rightarrow \mathbb{N}^{\mathcal{P}(\text{PG}(2,R))}$ as the extension of ϕ to multisets. For a multiset of points \mathfrak{K} in $\text{PHG}(2, R)$, the image $\Phi(\mathfrak{K})$ reduces \mathfrak{K} to the distribution of the points in \mathfrak{K} into the point classes of $\text{PHG}(2, R)$.

The strategy for the algorithm is to generate all possible images $\Phi(\mathfrak{K})$ up to $\text{PG}(2, \mathbb{F}_q)$ -isomorphism in a first step. In a second step, the preimages of these images are generated. Concerning the algorithmic complexity, the second step is much harder than the first one.

This approach suggests itself for several reasons: Without the intermediate step, the computations must be done under the full collineation group $\text{P}\Gamma\text{L}(3, R)$. But to compute the possible preimages of a given point class distribution \mathfrak{k} in the second step, the acting group is reduced to the preimage in $\text{P}\Gamma\text{L}(3, R)$ of the stabilizer of \mathfrak{k} by the Homomorphism Principle [17] and the fact that the mapping Φ naturally extends to a homomorphism of the group actions, mapping the action of $\text{P}\Gamma\text{L}(3, R)$ on $\mathcal{P}(\text{PHG}(2, R))$ to the action of $\text{P}\Gamma\text{L}(3, \mathbb{F}_q)$ on $\mathcal{P}(\text{PG}(2, \mathbb{F}_q))$. Furthermore, the next lemma (compare [6, Theorem 3.5]) summarizes severe restrictions on the possible point class distributions, which allow a drastic pruning of the search tree between the two steps:

Lemma 3.1 *Let \mathcal{H} be the projective Hjelmslev plane over R and assume that its factor plane \mathcal{G} is of odd order q . Let \mathfrak{K} be a 2-arc in \mathcal{H} .*

- (a) *Each 2-class is incident with a line class $[L]$ of multiplicity 2.*
- (b) *Each line class is incident with a point class of multiplicity 0.*
- (c) *If $u(\mathfrak{K}) = 2$, then $\#\mathfrak{K} \leq q^2 - q + 2$.*
- (d) *If $u(\mathfrak{K}) \geq 3$, then $\#\mathfrak{K} \leq q^2 - 2q + 3$.*
- (e) *If $u(\mathfrak{K}) \leq 2$, then each line class has multiplicity at most $q + 1$.*
- (f) *If $u(\mathfrak{K}) \leq 2$, then the number of 2-classes incident with a line class of multiplicity $q + 1$ is either $\frac{q-1}{2}$ or $\frac{q+1}{2}$.*

PROOF. To show part (a), let $[x]$ be a 2-class. Because \mathfrak{K} is a 2-arc, the line class determined by the 2 points in $[x]$ has multiplicity 2.

Let $[L]$ be a line class in \mathcal{H} . For each u -class $[x]$ on $[L]$ of multiplicity $u \geq 3$ we arbitrarily remove $u - 2$ points in $[x]$ from \mathfrak{K} . For the remaining point set \mathfrak{k} we have $\#(\mathfrak{k} \cap [x]) \leq 2$ for all point classes incident with $[L]$. In

the case $u(\mathfrak{K}) \leq 2$ it holds $\mathfrak{K} = \mathfrak{k}$. The multiset of points in $\Pi_{[L]}$ induced by $\mathfrak{k} \cap [L]$ is a 2-arc. Because q is odd, we get $\#(\mathfrak{k} \cap [L]) \leq q + 1$ which shows part (e). Furthermore, in the case $\#(\mathfrak{k} \cap [L]) = q + 1$ the induced multiset of points forms an oval in $\Pi_{[L]}$. The point ∞ is either external or internal to this oval, so the lines $L_{[x]} : x \in [L]$ through ∞ comprise either $\frac{q-1}{2}$ passants, 2 tangents, $\frac{q-1}{2}$ secants or $\frac{q+1}{2}$ passants, $\frac{q+1}{2}$ secants. Since the line segments on $L_{[x]}$ cover the point class $[x]$, parts (b) and (f) follow.

Now let $[x]$ be a point class of maximum multiplicity $u(\mathfrak{K})$. $\mathfrak{K} \cap [x]$ is a 2-arc in $\Pi_{[x]}$, so $u(\mathfrak{K}) = \#(\mathfrak{K} \cap [x]) \leq q + 1$. If $u(\mathfrak{K}) = 2$, then by part (a) there is a line class $[L]$ through $[x]$ with $\#([L] \setminus [x]) = 0$ and by part (e) each of the remaining q line classes through $[x]$ contain at most $q - 1$ points outside of $[x]$. This shows $\#\mathfrak{K} \leq 2 + q(q - 1) = q^2 - q + 2$, which is part (c).

If $u(\mathfrak{K}) = 3$, then the pairs of points in $\mathfrak{K} \cap [x]$ determine 3 line classes. Since \mathfrak{K} is a 2-arc, these line classes cannot contain any other point of \mathfrak{K} . Now let $[L]$ be one of the $q - 2$ remaining line classes incident with $[x]$, and $y \in \mathfrak{K} \cap [x]$. There are q lines in $[L]$ incident with y , and these lines cover $[L] \setminus [x]$. On each of these lines there is at most one further point of \mathfrak{K} . So we get $\#\mathfrak{K} \leq 3 + q(q - 2) = q^2 - 2q + 3$. Since q is odd, for $u(\mathfrak{K}) \geq 4$ the pairs of points in $\mathfrak{K} \cap [x]$ determine at least 4 line classes. The same reasoning leads to $\#\mathfrak{K} \leq u + q(q - 3) \leq (q + 1) + q(q - 3) = q^2 - 2q + 1$. This shows part (d). \square

Remark 1 For odd $q \geq 5$ each point of $\text{PG}(2, q)$ lies on at least 2 secants of a given oval. This shows that in the two cases of Lemma 3.1(f), the point set $\mathfrak{K} \cap [L]$ cannot be extended if we drop the condition $u(\mathfrak{K}) \leq 2$. This puts serious restrictions on the point class distribution of a line class $[L]$ of multiplicity $> q + 1$, which can be used to improve the bound in part (d) of the preceding Lemma.

In Theorem 5.1, this will be done explicitly for the chain rings \mathbb{Z}_{25} and \mathbb{S}_5 .

3.1 Creating the point class distributions

The first task for constructing all $(n, 2)$ -arcs in $\text{PHG}(2, \mathbb{Z}_{25})$ is the creation of all isomorphism types of point class distributions obeying the restrictions of Lemma 3.1. For the critical case $n = 22$, this can be done without the use of a computer:

Lemma 3.2 Let \mathfrak{K} be a $(22, 2)$ -arc in the projective Hjelmslev plane over \mathbb{Z}_{25} or \mathbb{S}_5 . The isomorphism type of the point class distribution $\Phi(\mathfrak{K})$ in the factor plane is given by one of the following cases:

(1) $u(\mathfrak{K}) = 1$.

(a) In the factor plane, the 0-classes are given by a line L and three collinear points not incident with L .

- (b) *In the factor plane, the 0-classes are given by a line L and three non-collinear points not incident with L .*
- (c) *The 0-classes form a projective triangle in the factor plane.*
- (2) *$u(\mathfrak{K}) = 2$, and there are six 2-classes forming an oval in the factor plane. The point pairs in the 2-classes determine the line classes tangent to the oval. The point classes internal to the oval are 1-classes, and the point classes external to the oval are 0-classes.*

PROOF. By Lemma 3.1(d), $u(\mathfrak{K}) \leq 2$. If $u(\mathfrak{K}) = 1$, by Lemma 3.1(b) the 0-classes form a blocking set of size $31 - 22 = 9$ in the factor plane. It is known that such a blocking set either contains a line, or it is isomorphic to a projective triangle. Using the fact that the collineation group of $\text{PHG}(2, R)$ acts transitively on the quadruples of points in general position, this gives the 3 isomorphism types listed in case (1).

Now we assume $u(\mathfrak{K}) = 2$. Let P_i be the set of all i -classes and $[x] \in P_2$ be a 2-class. By Lemma 3.1(a), one of the line classes incident with $[x]$ is of multiplicity 2, and by Lemma 3.1(e) the remaining 5 line classes incident with $[x]$ contain at most 6 points of \mathfrak{K} each. Because of $\#\mathfrak{K} = 22$, it follows that these 5 line classes contain exactly 6 points of \mathfrak{K} each, so by Lemma 3.1(f) each of these line classes is incident with one or two further 2-classes. This shows $6 \leq \#P_2 \leq 11$.

Let L_i denote the set of line classes incident with exactly i point classes in P_2 . We have seen that each point class $[y] \in P_2$ is incident with exactly 5 line classes in $L_2 \cup L_3$, so double counting the set of flags $([y], [L])$ with $[y] \in P_2$, $[L]$ incident with $[y]$ and $[L] \in L_2 \cup L_3$ gives the equation $5\#P_2 = 2\#L_2 + 3\#L_3$. Furthermore, double counting the pairs of point classes in P_2 shows $\binom{\#P_2}{2} = \#L_2 + 3\#L_3$. Solving this equation system for $(\#L_2, \#L_3)$ yields $2\#L_2 = \#P_2(11 - \#P_2)$ and $3\#L_3 = \#P_2(\#P_2 - 6)$. So $3 \mid \#P_2$ and therefore $\#P_2 \in \{6, 9\}$.

In the case $\#P_2 = 9$ it holds $\#P_1 = 4$ and $\#L_2 = \#L_3 = 9$. Let X be the set of all flags $([y], [L])$ with $[y] \in P_1$, $[L]$ incident with $[y]$ and $[L] \in L_2$. We count $\#X$ in two ways: Since all line classes in L_2 have multiplicity 6, each line class in L_2 is incident with exactly 2 point classes in P_1 . This shows $\#X = 2\#L_2 = 18$. On the other hand, because of $\#P_2 = 9$, a point class $[y] \in P_1$ is incident with at most 4 line classes in L_2 , which leads to the contradiction $\#X \leq 4\#P_1 = 16$.

So we get $\#P_2 = 6$ and $\#L_3 = 0$. This means that the point classes in P_2 form an oval in the factor plane. The only possibility for the line classes determined by the point pairs $\mathfrak{K} \cap [y]$, $[y] \in P_2$ are the line classes tangent to the oval P_2 . It follows that the 15 point classes external to P_2 are 0-classes. Because of $\#\mathfrak{K} = 22$, all the point classes internal to P_2 must be 1-classes.

□

Remark 2 (a) For the base ring \mathbb{Z}_{25} , the point class distributions (1a) and (1b) are not possible: Because there is an empty line class, such a $(22, 2)$ -arc would be contained in an affine subplane of $\text{PHG}(2, \mathbb{Z}_{25})$. But in [15] it was shown computationally that the maximum size of a 2-arc in $\text{AHG}(2, \mathbb{Z}_{25})$ is 20.

(b) While our main interest is in the projective Hjelmslev plane over \mathbb{Z}_{25} , Lemma 3.2 also holds for \mathbb{S}_5 . Let $\mathcal{H} = \text{PHG}(2, \mathbb{S}_5)$. The existence of a $(25, 2)$ -arc in \mathcal{H} implies the existence of a $(22, 2)$ -arc in \mathcal{H} realizing the point class distributions (1a) and (1b). Furthermore, the $(22, 2)$ -arc $\mathfrak{k}_{\mathbb{S}_5}$ in \mathcal{H} given in [9] realizes the point class distribution (2).

The automatic construction of the point class distribution is done by a backtracking search, checking the conditions of Lemma 3.1 in each step. Because only one representative of each isomorphism class is needed, we apply orderly generation [24]. Whenever a complete point class distribution \mathfrak{k} is found, all 2-arcs in its preimage in $\text{PHG}(2, \mathbb{Z}_{25})$ are created as described below. If in this search it turns out that even a smaller⁵ point class distribution $\mathfrak{k}' < \mathfrak{k}$ does not admit an $(n, 2)$ -arc in its preimage, it is clear that there does not exist an $(n, 2)$ -arc \mathfrak{K} with $\Phi(\mathfrak{K}) = \mathfrak{k}$. Thus \mathfrak{k}' , or even stronger all isomorphic copies of \mathfrak{k}' , are a *forbidden substructure* for the point class distributions of an $(n, 2)$ -arc. This restriction on the point class distributions is not covered by Lemma 3.1 and can be used additionally for the ongoing construction of point class distributions.

3.2 Lifting point class distributions to 2-arcs in $\text{PHG}(2, \mathbb{Z}_{25})$

After the generation of a possible point class distribution, the preimages in the Hjelmslev plane are built. Starting from $\mathfrak{K} = \emptyset$ we iteratively extend \mathfrak{K} point-wise, with respect to the point class distribution \mathfrak{k} and the 2-arc property. To make our computation more efficient we construct the possible point sets only up to isomorphism. For the isomorphism test we use a combination of orderly generation [24] and the ladder game, based on the homomorphism principle [16, 25, 17].

The orderly generation algorithm needs an assignment of the predicate *canonical* to exactly one representative in each orbit. The two-step approach also works for the computation of a canonical representative: Having such a predicate in the factor plane $\text{PG}(2, \mathbb{Z}_5)$ together with the homomorphism of group actions Φ , by the Homomorphism Principle we are able to arrange the definition of canonicity in $\mathbb{N}^{\mathcal{P}(\text{PHG}(2, \mathbb{Z}_{25}))}$ in such a way that the image of a canonical point set under the mapping Φ is always canonical. Furthermore by the Homomorphism Principle the search space for the canonical candidate can be reduced: For a point set \mathfrak{K} in the preimage of a canonical point class

⁵The common partial order on multisets is used.

distribution \mathfrak{k} , the canonical form of \mathfrak{K} must be in the orbit of \mathfrak{K} under the Φ -preimage of the stabilizer of \mathfrak{k} in $\text{PTL}(3, \mathbb{Z}_5)$. This group usually is much smaller than the full group $\text{PTL}(3, \mathbb{Z}_{25})$.

These methods were implemented in C++ and executed on a single CPU of type Intel Xeon E5520. Running the program for $(22, 2)$ -arcs in $\text{PHG}(2, \mathbb{Z}_{25})$ took 8.5 hours and gave no result. Running the program for $(21, 2)$ -arcs took 13.5 hours and returned exactly one $(21, 2)$ -arc, the arc already found in [9]. This proves Theorem 1.1.

4 Computation via the extension of 2-arcs in the affine plane

Now we follow a different approach: First the $(20, 2)$ - and $(19, 2)$ -arcs in the affine plane $\text{AHG}(2, \mathbb{Z}_{25})$ are classified and then tested for extendability to a $(22, 2)$ - respectively $(21, 2)$ -arc in $\text{PHG}(2, \mathbb{Z}_{25})$. This is justified by the following lemma:

Lemma 4.1 *Let \mathfrak{K} be a 2-arc in the projective Hjelmslev plane over \mathbb{Z}_{25} or \mathbb{S}_5 with $u(\mathfrak{K}) \leq 2$. Then there is a line class of multiplicity at most 2. Thus by removing this line class, it remains a 2-arc in $\text{AHG}(2, R)$ of size at least $\#\mathfrak{K} - 2$.*

PROOF. If there exists a 2-class, a suitable line class is given by Lemma 3.1(a). Now assume $u(\mathfrak{K}) = 1$. Let $a_i, i \in \{0, \dots, 6\}$ be the spectrum of the 1-classes in the factor plane, that is a_i denotes the number of line classes incident with exactly i 1-classes. Because of Lemma 3.1(b), we get $a_6 = 0$.

Now we assume $a_0 = a_1 = a_2 = 0$. So the standard equations on the spectrum are $a_3 + a_4 + a_5 = 31$, $3a_3 + 4a_4 + 5a_5 = 6\#\mathfrak{K}$ and $3a_3 + 6a_4 + 10a_5 = \binom{\#\mathfrak{K}}{2}$. Solving this system of equations yields $a_4 = -\#\mathfrak{K}^2 + 43\#\mathfrak{K} - 465 = -(\#\mathfrak{K} - \frac{43}{2})^2 - \frac{11}{4} < 0$, which is a contradiction. This shows that there is a line class of multiplicity at most 2. \square

4.1 Canonization in $\text{AHG}(2, \mathbb{Z}_{25})$

First we outline how to efficiently determine a canonical representative in $\text{AHG}(2, \mathbb{Z}_{25})$ of a point set \mathfrak{K} which contains a point triple in general position (no 2 points in the same point class, no 3 points in the same line class).⁶ By the map mapping $(x, y) \mapsto x + 25y$, computed in the integers, we can compare points. Sets of points are compared by the lexicographic ordering. The smallest point set isomorphic to \mathfrak{K} is called *canonical* form of \mathfrak{K} . Because \mathfrak{K} contains a triple of points in general position, the canonical form of \mathfrak{K}

⁶This is not a hard restriction: Every 2-arc \mathfrak{K} with $\#\mathfrak{K} \geq 7$ and $\#(\mathfrak{K} \cap [x]) \leq 2$ for all point classes $[x]$ contains a triple of points in general position.

fulfills $\left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \subset \mathfrak{K}$ (the points correspond to the integers 0, 1, and 25).

In order to efficiently canonize \mathfrak{K} with respect to $\text{AGL}(2, \mathbb{Z}_{25})$ we loop over all triples $\mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3 \in \mathfrak{K}$ in general position, set $\mathbf{b} = -\mathbf{k}_1$, and uniquely determine \mathbf{A}' via $\mathbf{A}'(\mathbf{k}_2 - \mathbf{k}_1) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\mathbf{A}'(\mathbf{k}_3 - \mathbf{k}_1) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, where we use the notation from subsection 2.4.⁷ Thus we obtain a canonizer which needs at most $\#\mathfrak{K}^3$ operations. We can easily extend this to a canonizer for $\text{PGL}(3, \mathbb{Z}_{25}) \downarrow$ by looping over all 25 possibilities for \mathbf{c} and determining \mathbf{A}' via $\mathbf{A}'(\mathbf{k}_2 - \mathbf{k}_1) = \begin{pmatrix} 1 + \mathbf{c}(x, y)^T \\ 0 \end{pmatrix}$, $\mathbf{A}'(\mathbf{k}_3 - \mathbf{k}_1) = \begin{pmatrix} 0 \\ 1 + \mathbf{c}(x, y)^T \end{pmatrix}$. If we have an arc \mathfrak{K} which is canonical with respect to $\text{PGL}(3, \mathbb{Z}_{25}) \downarrow$ we can also revert these steps to obtain a complete list of 25 arcs which are isomorphic to \mathfrak{K} and canonical with respect to $\text{AGL}(2, \mathbb{Z}_{25})$.

4.2 Classification of arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ by orderly generation and integer linear programming

The classification of arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ is explained at the example of the $(20, 2)$ -arcs. We use an orderly generation approach (see [24]), where we utilize integer linear programming to prune the search tree. Each $(20, 2)$ -arc \mathfrak{K} in $\text{AHG}(2, \mathbb{Z}_{25})$ corresponds to a solution of the binary linear program (BLP)

$$\begin{aligned} \sum_{i \in \mathcal{P}(\text{AHG}(2, \mathbb{Z}_{25}))} x_i &\geq 20 \\ \sum_{i \in L} x_i &\leq 2 \quad \forall L \in \mathcal{L}(\text{AHG}(2, \mathbb{Z}_{25})) \\ x_i &\in \{0, 1\} \quad \forall i \in \mathcal{P}(\text{AHG}(2, \mathbb{Z}_{25})), \end{aligned}$$

via $\mathfrak{K} = \{i \in \mathcal{P}(\text{AHG}(2, \mathbb{Z}_{25})) \mid x_i = 1\}$. Due to symmetry and the large integrality gap, this BLP can not be solved directly using customary ILP solvers like `ILOG CPLEX`. To deal with the large automorphism group, one possibility would be to apply techniques e. g. from [19]. We chose another possibility: By fixing some x_i to one, i. e. by prescribing some points of \mathfrak{K} , the biggest part of the symmetries is broken and we can try to solve the resulting BLP in reasonable time. Of course for the search to be complete, all the non-isomorphic possibilities of prescribing some x_i must be dealt with separately.

We can utilize this approach to deduce that for all point classes $[x]$ it holds $\#(\mathfrak{K} \cap [x]) \in \{0, 1\}$ as follows. First we assume that \mathfrak{K} contains

⁷The matrix \mathbf{A}' does not exist in the cases where $\mathbf{k}_1, \mathbf{k}_2$ and \mathbf{k}_3 are not in general position.

some points k_1, \dots, k_6 with $\phi(k_i) = \phi(k_j)$ if and only if either $i = j$ or $\{i, j\} \in \left\{ \{1, 2\}, \{3, 4\}, \{5, 6\} \right\}$, i. e. there are at least three 2-classes. For each of the 104, with respect to $\text{AGL}(2, \mathbb{Z}_{25})$, non-isomorphic such subsets $\{k_1, \dots, k_6\}$ we check that the corresponding BLP is infeasible. Thus by now we know that a $(20, 2)$ -arc in $\text{AHG}(2, \mathbb{Z}_{25})$ can have at most two 2-classes.

Next we prescribe points k_1, \dots, k_5 , where $\phi(k_i) = \phi(k_j)$ if and only if either $i = j$ or $\{i, j\} \in \left\{ \{1, 2\}, \{3, 4\} \right\}$. Here there are only 18, with respect to $\text{AGL}(2, \mathbb{Z}_{25})$, non-isomorphic possibilities. To forbid a third 2-class we add the inequalities

$$\sum_{i \in \mathcal{C}} x_i \leq 1 \quad \forall \mathcal{C} \in \left\{ [k] : k \in \mathcal{P}(\text{AHG}(2, \mathbb{Z}_{25})) \right\} \setminus \left\{ [k_1], [k_3] \right\}$$

to the BLP. Again it turned out that there are no feasible solutions. In the final step we we prescribe points k_1, \dots, k_5 , where $\phi(k_i) = \phi(k_j)$ if and only if either $i = j$ or $\{i, j\} = \{1, 2\}$. In all 185, with respect to $\text{AGL}(2, \mathbb{Z}_{25})$, non-isomorphic cases the corresponding BLP is infeasible.

In the following we can assume $\#(\mathfrak{K} \cap [x]) \in \{0, 1\}$ for all point classes $[x]$. As a new ingredient we utilize the concept of orderly generation, i. e. if we prescribe a set \mathfrak{K}' of points then we only search for arcs \mathfrak{K} , where \mathfrak{K} is lexicographically minimal with respect to $\text{AGL}(2, \mathbb{Z}_{25})$, i. e. where $\mathfrak{K} \leq \psi(\mathfrak{K})$ for all automorphisms $\psi \in \text{AGL}(2, \mathbb{Z}_{25})$, and where the smallest $\# \mathfrak{K}'$ elements of \mathfrak{K} are equal to \mathfrak{K}' . To this end we can formulate some necessary linear constraints: If for given \mathfrak{K}' there are points $j \in \mathfrak{K}'$, $i \in \mathcal{P}(\text{AHG}(2, \mathbb{Z}_{25}))$ and an automorphism ψ such that $\psi\left(\{i\} \cup \mathfrak{K}' \setminus \{j\}\right) < \mathfrak{K}'$ then we can add the constraint

$$x_i = 0$$

to our BLP. If there are points $j_1 \neq j_2 \in \mathfrak{K}'$, $i_1 \neq i_2 \in \mathcal{P}(\text{AHG}(2, \mathbb{Z}_{25}))$ and an automorphism ψ such that $\psi\left(\{i_1, i_2\} \cup \mathfrak{K}' \setminus \{j_1, j_2\}\right) < \mathfrak{K}'$ then we can add the constraint

$$x_{i_1} + x_{i_2} \leq 1$$

to the BLP. Using these constraints we were able to drastically reduce the number of lexicographically smallest sets $\mathfrak{K}' = \{k_1, \dots, k_5\}$ which possibly can be extended to $(20, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ using the feasibility of the BLP. For each such *partial* arc \mathfrak{K}' we can easily determine a set \mathfrak{K}'' of points such that we have $\mathfrak{K} \cap \mathfrak{K}'' = \emptyset$ for all lexicographically minimal $(20, 2)$ -arcs \mathfrak{K} with $\mathfrak{K}' \subset \mathfrak{K}$. (This set consists of the $i \in \mathcal{P}(\text{AHG}(2, \mathbb{Z}_{25}))$ where we would add $x_i = 0$ to the BLP.)

After these preparative calculations we have classified the $(20, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ using a branch&bound approach as follows. We start with one

of the \mathfrak{R}' , where the points from the corresponding sets \mathfrak{R}'' are forbidden, as described above, and extend the partial arcs point by point by branching on the point classes $[x]$. (See [13] for the question where to branch.) I. e. for a given point class $[x]$ we loop over all possibilities to extend the current partial arc with a point from $[x]$ or to take none of the points from $[x]$.

In the bounding step we perform two checks. If the cardinality of the partial arc \mathfrak{R} is either at most 8 or 20 we check whether there is an automorphism $\psi \in \text{AGL}(2, \mathbb{Z}_{25})$ such that the smallest five elements of $\psi(\mathfrak{R})$ are lexicographically smaller than the initial \mathfrak{R}' , see Subsection 4.1 for the details. If such a ψ exists, we can prune the search tree (isomorphism-pruning). For the other check we count the number e of point classes $[x]$, where there is a point $k \in [x] \setminus (\mathfrak{R} \cup \mathfrak{R}'')$ such that $\mathfrak{R} \cup \{k\}$ is a 2-arc. If $\#\mathfrak{R} + e < 20$ we can prune the search tree. (The latter bound relies on the fact that we only have to consider arcs without 2-classes.)

The maximum size of a 2-arc in $\text{AHG}(2, R)$ is 20, this was determined computationally in [15]. Now we can give the number of such $(20, 2)$ arcs up to different automorphism groups: In Table 1 we give the number of non-isomorphic $(20, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ per size of its stabilizer Aut_1 in $\text{AGL}(2, \mathbb{Z}_{25})$ (collineations of $\text{AHG}(2, \mathbb{Z}_{25})$ preserving the standard parallelism), Aut_2 in $\text{PGL}(3, \mathbb{Z}_{25}) \downarrow$ (all collineations of $\text{AHG}(2, \mathbb{Z}_{25})$) and Aut_3 in $\text{PGL}(3, \mathbb{Z}_{25})$ (all collineations of $\text{PHG}(2, \mathbb{Z}_{25})$, via the standard embedding). We verified that none of these arcs can be extended to a $(22, 2)$ -arc in $\text{PHG}(2, \mathbb{Z}_{25})$.

In fact, all these $(20, 2)$ -arcs are maximal in $\text{PHG}(2, \mathbb{Z}_{25})$. This is consistent with our main result that the $(21, 2)$ -arc in $\text{PHG}(2, \mathbb{Z}_{25})$ is unique, because all line classes of the $(21, 2)$ -arc contain at least two points of this arc.

$\# \text{Aut}_\star$	1	2	4	Σ
$\# \text{Aut}_1$	11198	226	6	11430
$\# \text{Aut}_2$	420	62	6	488
$\# \text{Aut}_3$	415	47	4	466

Table 1: Number of non-isomorphic $(20, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ per size of the automorphism group.

In the same way, the $(19, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ were generated up to isomorphism. Interestingly enough, it turns out that a $(19, 2)$ -arc in $\text{AHG}(2, \mathbb{Z}_{25})$ has no or exactly four 2-classes. The results of the former case are summarized in Table 2. In the latter case there are exactly 75, 3, 3 non-isomorphic (with respect to the different automorphism groups) solutions, each with trivial stabilizer in $\text{PGL}(3, \mathbb{Z}_{25})$.

A check for extendability revealed that among the $157213+3 \text{ PGL}(3, \mathbb{Z}_{25}) \downarrow$ -

# Aut _★	1	2	3	Σ
# Aut ₁	3922099	2555	33	3924687
# Aut ₂	156669	511	33	157213
# Aut ₃	146610	511	33	147154

Table 2: Number of non-isomorphic $(19, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ with maximum point class multiplicity 1.

representatives of $(19, 2)$ -arcs in $\text{AHG}(2, \mathbb{Z}_{25})$ there is only a single arc \mathfrak{K} which is extendable to a $(21, 2)$ -arc in $\text{PHG}(2, \mathbb{Z}_{25})$. Furthermore, the extension of \mathfrak{K} is unique up to isomorphism, so together with Lemma 4.1 this proves Theorem 1.1.

More precisely, \mathfrak{K} is given by

$$\{(0, 0), (0, 1), (15, 12), (20, 3), (15, 4), (1, 0), (1, 1), (6, 12), (21, 9), (2, 15), \\ (12, 3), (3, 11), (3, 2), (8, 14), (9, 10), (14, 11), (4, 2), (4, 13), (14, 19)\}.$$

By the standard embedding in $\text{PHG}(2, \mathbb{Z}_{25})$, \mathfrak{K} can be extended by the points

$$(20 : 1 : 5) \quad \text{and} \quad (5 : 1 : 7).$$

The uniqueness of \mathfrak{K} necessarily means that all affine subsets of size 19 of the unique $(21, 2)$ -arc \mathfrak{k} in $\text{PHG}(2, \mathbb{Z}_{25})$ are isomorphic. Again this is consistent with the analysis of \mathfrak{k} given in [9]: \mathfrak{k} has maximum point class multiplicity $u(\mathfrak{k}) = 1$, and in the factor plane the 0-classes form a projective triangle Δ extended by the unique fixed point under the action of the stabilizer of Δ on the factor plane. Therefore, there are 3 possibilities for the choice of a line class at infinity, namely the 3 edges of the projective triangle. Under the stabilizer of \mathfrak{k} which has order 3, these three line classes are in the same orbit.

5 Further results

5.1 Number of non-isomorphic $(n, 2)$ -arcs for large n

We used the same methods to compute further numbers of isomorphism types of 2-arcs. Wherever possible, both computational approaches were used to assure the correctness of the result.

Table 3 shows the number of $\text{PGL}(3, \mathbb{Z}_{25})$ -isomorphism types of $(n, 2)$ -arcs in $\text{PHG}(2, \mathbb{Z}_{25})$. The column s_i lists the number of $(n, 2)$ -arcs whose stabilizer has size i , and the column Σ lists the numbers of all $(n, 2)$ -arcs. In the column "time", the running time of the algorithm described in Section 3 is given.

Remarkably, the stabilizers of large 2-arcs in $\text{PHG}(2, \mathbb{Z}_{25})$ are relatively small. For comparison we mention that in $\text{PHG}(2, \mathbb{S}_5)$ there exists a $(25, 2)$ -arc whose stabilizer has order 300. This implies that using the method of prescribed automorphisms like in [11], a 2-arc of size at least 18 in $\text{PHG}(2, \mathbb{Z}_{25})$ is much harder to find than a $(25, 2)$ -arc in $\text{PHG}(2, \mathbb{S}_5)$.

n	s_1	s_2	s_3	s_4	s_6	s_8	s_{12}	s_{24}	Σ	time
22									0	30002s
21			1						1	47750s
20	591	63		4					658	155258s
19	221374	687	71						222132	487340s
18	23880140	16842	721	271	73	11	9	4	23897599	2299265s

Table 3: Number of non-isomorphic $(n, 2)$ -arcs in $\text{PHG}(2, \mathbb{Z}_{25})$.

5.2 The maximum size of a 2-arc of given maximum point class multiplicity

Using a combination of the computational results and geometric reasoning, we are ready to determine the maximum size of a 2-arc \mathfrak{K} in $\text{PHG}(2, \mathbb{Z}_{25})$ and $\text{PHG}(2, \mathbb{S}_5)$ of a given maximum point class multiplicity $u(\mathfrak{K})$:

Theorem 5.1 *Let $u \in \{1, \dots, q+1\}$ and $m_{2,u}(R)$ be the maximum size of a 2-arc \mathfrak{K} in $\text{PHG}(2, R)$ with $u(\mathfrak{K}) = u$.*

For $R \in \{\mathbb{Z}_{25}, \mathbb{S}_5\}$ the values of $m_{2,u}(R)$ are:

R	u					
	1	2	3	4	5	6
\mathbb{Z}_{25}	22	19	12	12	10	6
\mathbb{S}_5	25	22	12	12	10	6

PROOF. Let P_u be the set of all u -classes and x be a u -class.

For a line class $[L]$, the non-increasing sequence of the multiplicities of the point classes incident with $[L]$ is called *type* of $[L]$. The type of $[L]$ is a partition of the multiplicity of $[L]$ into 6 summands. In the following, we assume the usual partial order on the set of partitions.

By Lemma 3.1(f), types greater or equal to $(2, 1, 1, 1, 1, 0)$ or greater or equal to $(1, 1, 1, 1, 1, 1)$ are impossible, and by the argument in Remark 1, types greater than $(2, 2, 1, 1, 0, 0)$ or greater than $(2, 2, 2, 0, 0, 0)$ are impossible.

Furthermore, types greater or equal to $(3, 3, 1, 0, 0, 0)$ are impossible: Assume that there is a line class $[L]$ of type $(3, 3, 1, 0, 0, 0)$. Let x be the point of \mathfrak{K} corresponding to the entry 1 in the type. All lines of $\Pi_{[L]}$ incident with

x contain at most 2 points of the induced point set \mathfrak{k} , and the line incident with x and p_∞ intersects \mathfrak{k} only in x . This gives $\#\mathfrak{k} \leq 6$, a contradiction.

For $u = 6$, it is clear that the points of \mathfrak{K} in $[x]$ must form an oval, and no further point can be added to \mathfrak{K} .

For $u = 5$, the points in $[x]$ determine all but possibly one line class $[L]$ incident with $[x]$. To get a 2-arc \mathfrak{K} , at most one further point class $[y]$ can have non-empty intersection with \mathfrak{K} , and $[y]$ must be incident with $[L]$. So $\#\mathfrak{K} \leq 10$. If we arrange the points of \mathfrak{K} within $[x]$ and $[y]$ such that they do not determine $[L]$, we get indeed a $(10, 2)$ -arc, showing $m_{2,5}(R) = 10$.

For $u = 4$, each 4-class $[y]$ is incident with at most 2 line classes not determined by $[y]$. By the restrictions on the types, no three 4-classes are collinear. So $\#P_4 \leq 3$. For $\#P_4 = 3$, all point classes not in P_4 are 0-classes. Furthermore, it is easy to see that there is indeed a $(12, 2)$ -arc of this structure. For $\#P_4 = 2$, let $P_4 = \{[x], [y]\}$. The line class $[L]$ incident with $[x]$ and $[y]$ must be of type $(4, 4, 0, 0, 0, 0)$. Outside of $[L]$ there is at most one point class of non-zero multiplicity, so $\#\mathfrak{K} \leq 2 \cdot 4 + 3 = 11$. For $\#P_4 = 1$ the restrictions on the types show that a line class incident with $[x]$ has multiplicity at most 7, which gives $\#\mathfrak{K} \leq 4 + 2 \cdot (7 - 4) = 10$.

Now assume $u = 3$. Again, no three 3-classes are collinear. Each 3-class is incident with at least three line classes of multiplicity 3. So if there are three non-collinear 3-classes, there is at most one further point class which is not a 0-class. This leads to $\#\mathfrak{K} \leq 4 \cdot 3 = 12$, and it is straightforward to check that there is a $(12, 2)$ -arc of this structure. For $\#P_3 = 2$, the line class $[L]$ incident with the two 3-classes must be of type $(3, 3, 0, 0, 0, 0)$. Outside of $[L]$ there remain at most 4 point classes $[x_i]$ which are not a 0-class. There are 4 line classes through a 3-class and two distinct point classes $[x_i], [x_j]$. Since the type $(3, 2, 2, 0, 0, 0)$ is not possible, at most 2 of the point classes $[x_i]$ can be 2-classes. In total, $\mathfrak{K} \leq 2 \cdot 3 + 2 \cdot 2 + 2 \cdot 1 = 12$. In the case $\#P_3 = 1$, by the restrictions on the types the line classes incident with $[x]$ have multiplicity at most 6, so again $\#\mathfrak{K} \leq 3 + 3 \cdot (6 - 3) = 12$.

The values $m_{2,u}(\mathbb{Z}_{25})$ for $u \in \{1, 2\}$ follow from the computer classification in this article. $m_{2,2}(\mathbb{S}_5) = 22$ follows from the existence of the $(22, 2)$ -arc over \mathbb{S}_5 given in [9] and Lemma 3.1(c). Finally, the value $m_{2,1}(\mathbb{S}_5) = 25$ follows from [4]. \square

References

- [1] A. Cronheim, *Dual numbers, Witt vectors, and Hjlemslev planes*, Geom. Dedicata **7** (1978), 287–302.
- [2] L. Hemme, D. Weijand, *Arcs in projektiven Hjlemslev-Ebenen*, Fortgeschrittenenpraktikum, Technische Universität München, 1999.

- [3] T. Honold, M. Kiermaier, *Classification of maximal arcs in small projective Hjelmslev geometries*, in "Proceedings of the Tenth International Workshop on Algebraic and Combinatorial Coding Theory 2006", (2006), 112–117.
- [4] T. Honold, M. Kiermaier, *The existence of maximal $(q^2, 2)$ -arcs in uniform projective Hjelmslev planes over chain rings of odd prime characteristic*, in preparation, 2010.
- [5] T. Honold, I. Landjev, *Linear codes over finite chain rings*, Electr. J. Comb. **7** (2000), #R11.
- [6] T. Honold, I. Landjev, *On arcs in projective Hjelmslev planes*, Discrete Math. **231** (2001), 265–278.
- [7] T. Honold, I. Landjev, *On maximal arcs in projective Hjelmslev planes over chain rings of even characteristic*, Finite Fields Appl. **11** (2005), 292–304.
- [8] M. Kiermaier, *Arcs und Codes über endlichen Kettenringen*, Diploma thesis, Technische Universität München, 2006.
- [9] M. Kiermaier, M. Koch, *New complete 2-arcs in the uniform projective Hjelmslev planes over chain rings of order 25*, in "Proceedings of the Sixth International Workshop on Optimal Codes and Related Topics 2009", (2009), 206–113.
- [10] M. Kiermaier, A. Kohnert, *Online tables of arcs in projective hjelmslev planes*, www.algorithm.uni-bayreuth.de.
- [11] M. Kiermaier, A. Kohnert, *New arcs in projective Hjelmslev planes over Galois rings*, in "Proceedings of the Fifth International Workshop on Optimal Codes and Related Topics 2007", (2007), 112–119.
- [12] W. Klingenberg, *Projektive und affine Ebenen mit Nachbarelementen*, Math. Z. **60** (1954), 384–406.
- [13] D. E. Knuth, *Estimating the efficiency of backtrack programs*, Math. Comput. **29** (1975), 121–136.
- [14] A. Kreuzer, *Projektive Hjelmslev-Räume*, Ph.D. thesis, Technische Universität München, 1988.
- [15] S. Kurz, *Caps in \mathbb{Z}_n^2* , Serdica J. Comput. **3** (2009), 159–178.
- [16] R. Laue, *Construction of combinatorial objects – a tutorial*, Bayreuther Math. Schr. **43** (1993), 53–96.

- [17] R. Laue, *Constructing objects up to isomorphism, simple 9-designs with small parameters*, in "Algebraic Combinatorics and Applications" (Berlin, Heidelberg, New York), Springer, (2001), 232–260.
- [18] H. Lüneburg, *Affine Hjelmslev-Ebenen mit transitiver Translationsgruppe*, Math. Z. **79** (1962), 260–288.
- [19] F. Margot, *Pruning by isomorphism in branch-and-cut*, Math. Programming **94** (2002), 71–90.
- [20] B. McKay, *nauty, Version 2.2*, (<http://cs.anu.edu.au/~bdm/nauty/>).
- [21] A. A. Nečaev, *Finite principal ideal rings*, Math. USSR-Sb. **20** (1973), 364–382.
- [22] A. A. Nechaev, *Finite rings with applications*, in "Handbook of Algebra" (M. Hazewinkel, ed.), vol. 5, Elsevier Science Publishers, (2008), 213–320.
- [23] R. Raghavendran, *Finite associative rings*, Composito Math. **21** (1969), 195–229.
- [24] R. C. Read, *Every one a winner or how to avoid isomorphism search when cataloguing combinatorial configurations*, Ann. Discrete Math. **2** (1978), 107–120.
- [25] B. Schmalz, *The t -designs with prescribed automorphism group, new simple 6-designs*, J. Comb. Des. **1** (1993), 125–170.

E-mail address: michael.kiermaier@uni-bayreuth.de

E-mail address: matthias.koch@uni-bayreuth.de

E-mail address: sascha.kurz@uni-bayreuth.de